

**Kamala Education Society's
Pratibha College of Commerce & Computer Studies, Chinchwad, Pune-19**



**A
Project Report
On
“Data Security using Cryptography”**

**Developed by,
4855: Master. Aadesh Patil
4803: Miss. Disha Dharmadhikari**

**T.Y.B.B.A. (C.A.)
Under
Savitribai Phule Pune University
(2021-2022)**

**Kamala Education Society's
Pratibha College of Commerce & Computer Studies, Chinchwad, Pune-19**



Certificate

This is to certify that **Master. Aadesh Patil & Miss Disha Dharmadhikari** have satisfactorily completed the **JAVA PROJECT** entitled “**DATA SECURITY USING CRYPTOGRAPHY**” for **T.Y.B.B.A.(C.A.) Semester V CA-505 Project** under the **Savitribai Phule Pune University** in the academic year **2021-2022**.

Dr. Babasaheb Sangale
Principal

Mrs. Hemalata Chavan
Program Coordinator

Mrs. Ashlesha Deole
Project Guide

Internal Examiner

External Examiner

Date:

ACKNOWLEDGEMENT

Any efforts to produce successful creation require the help, Guidance and support of many people and their experience. We would like to express our sincere and heartfelt gratitude to all of them.

We would like to take this opportunity to thanks all the people who have directly or indirectly helped this project. We would like to thank our guide. Prof. Ashlesha Deole, for her valuable guidance.

Date:

-Master. Aadesh Patil

-Miss. Disha Dharmadhikari

Index

Sr. No	Contents	Page No.
1	Introduction	1-4
1.1	Motivation	
1.2	Problem Statement	
1.3	Purpose/Objective and Goals	
1.4	Project Scope and Limitations	
2	System analysis	5-7
2.1	Existing systems	
2.2	Scope and Limitations of Existing Systems	
2.3	Project Perspective, Features	
2.4	Stakeholders	
2.5	Requirement Analysis	
2.5.1	Functional Requirements	
2.5.2	Non–Functional Requirements	
2.5.3	Performance Requirements	
2.5.4	Security Requirements	

3	System Design	7-14
3.1	Design constraints	
3.2	System Model: DFD	
3.3	ER Diagram	
3.4	Use case Diagram	
3.5	Class Diagram	
3.6	Activity Diagram	
3.7	Sequence Diagram	
3.8	Data Dictionary	
3.9	User Interfaces	
4	Implementation details	15-16
4.1	Software/Hardware Specifications	
5	Outputs and Reports Testing	17-27
5.1	Unit Test	
5.2	Integration Study	
5.3	Test case	
5.4	System Testing	
5.5	Sample Input & Output Screen	
6	Conclusion	28
7	Future Enhancement	29

8	Bibliography and References	30
----------	------------------------------------	-----------

1. Introduction

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

While cryptography is the science of securing data, cryptanalysis is the science of analysing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination.

A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key — a word, number, or phrase — to encrypt the plaintext. The same plaintext encrypts to different ciphertext with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key.

1.1 Motivation

Until recently, encryption was primarily used by companies to prevent reputational and financial damage. By encrypting sensitive items such as medical records, emails and corporate documents, organizations put themselves in a good position to avoid embarrassing revelations that could drive away customers, run afoul of applicable regulations or give a leg up to competitors.

For now, many organizations lack dedicated staff for key management and encryption policy enforcement. Adding these personnel, or working with a security provider, could help to get implementation efforts on track.

1.2 Problem Statement:

The Purpose of this project is to provide the correct data with security to the user. For some of the users that it might be lost during the translation process in the network and for some, the data might be changed by the unauthorised person on the network at there are some other security problems in the network. Our application will give you more security to the data present in the network and there will be able to reduce the loss of data and network which will be transmitted for the sender to receiver using latest Technologies. Only the Authorised person that is who are using our application will there in the network. Purpose algorithms is to hide the audio data effectively in an image without any suspicion of the data being hidden in the image. It is the work against the attacked by using a distinct new image that isn't possible to compress.

The aim of the project is to hide the data in an image using Cryptography and ensure that the quality of concealing data must not be lost.

We use a method for hiding the data in distinct image file to securely send over the network without any for suspicious data being hidden. This algorithm required a distinct image which we can use as a carrier and hide the data which is well within the limits of threshold that the image can hide, that will secure the data.

1.3 Purpose/Objective and Goals

Cryptography is the practice and study of techniques for secure communication in the presence of third parties. More generally, it is about constructing and analysing protocols that overcome the influence of attackers or outside people, and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Applications of cryptography include ATM cards, computer passwords.

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

Objectives:

- For Automatic translation from natural specifications
- For Automatic security awareness, analysis, and correction
- For Automatic optimization for diverse platforms:
- To Enable knowledge transfer and exploitation:
- To Support security critical ICT projects:
- To Establish and develop research theme

Goals:

- Data Privacy(confidentiality)
- Data Authenticity (it came from where it claims)
- Data integrity (it has not been modified on the way) in the digital world

1.4 Project Scope and Limitations

Scope:

This project aims at converting the plaintext into a form unreadable by unauthorized people and hence can be readily transferred across the web and decrypted at the recipient side only by authorized people. To provides an interactive environment to encrypt, decrypt or transfer encrypted files without compromising with the integrity and privacy of critical information.

In the era of wide area, open distributed systems, this system will help resolve various security issues.

Limitation:

- A strongly encrypted, authentic, and digitally signed information can be **difficult to access even for a legitimate user** at a crucial time of decision-making. The network or the computer system can be attacked and rendered non-functional by an intruder.
- **High availability**, one of the fundamental aspects of information security, cannot be ensured using cryptography. Other methods are needed to guard against the threats such as denial of service or complete breakdown of information system.
- Another fundamental need of information security of **selective access control** also cannot be realized using cryptography. Administrative controls and procedures are required to be exercised for the same.
- Cryptography does not guard against the vulnerabilities and **threats that emerge from the poor design of systems**, protocols, and procedures. These need to be fixed through proper design and setting up of a defensive infrastructure.

- Cryptography comes at cost. The cost is in terms of time and money
- Addition of cryptographic techniques in the information processing leads to delay.
- The use of public key cryptography requires setting up and maintenance of public key infrastructure requiring the handsome financial budget.
- The security of cryptographic technique is based on the computational difficulty of mathematical problems. Any breakthrough in solving such mathematical problems or increasing the computing power can render a cryptographic technique vulnerable.

2. System analysis

2.1 Existing system

- There is no option to try all the algorithms together in one system.
- There is no privilege for the user to send the encrypted message to other person as a mail.
- There is no database storage for the existing system. Further retrieval of the code is not possible.
- The system does not check for any authentication. Any user can encrypt and decrypt.
- It is easy for an intruder (third party) to access the text and he can make his own changes in it.

2.2 Scope and Limitations of Existing Systems

- The algorithms used in classical cryptography are not completely free from loopholes. As a result of such loopholes, the hackers can use it to crack the encrypted information and then use the same to perform all sorts of unethical activities.
- The key size used, and classical cryptography is comparatively smaller. Resulting, reduces the life expectancy of the algorithms.
- Classical Cryptography is easier to implement, but it requires massive computation to make the algorithms effective.
- The one-time pad is a cumbersome way of encrypting and requires a personal meeting for the exchange of the pads.
- If you're using classical cryptography without the use of OTP, all individuals having proper knowledge in cryptography will be able to crack your code and extract all information.

2.3 Project Perspective, Features

Features:

- **Confidentiality:**
Information can only be accessed by the person for whom it is intended and no other person except him can access it.
- **Integrity:**
Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
- **Non-repudiation:**
The creator/sender of information cannot deny his or her intention to send information at later stage.
- **Authentication:**
The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

2.4 Requirement Analysis

HARDWARE REQUIREMENTS

- 64-bit architecture.
- 2+ GHz CPU.
- 8 GB RAM.
- At least 60 GB of hard disk space available.

SOFTWARE REQUIREMENTS

- Spring Tool Suite 4
- Angular 8
- JAVA
- Node 14
- VS Code
- Amazon Web Services Server

2.4.1 Functional Requirements

Functional requirement describes activities and services that must provide:

- An Admin must have good knowledge **of computer systems**
- An only user must be able to use the system.
- A Cryptographer must have good **knowledge of networking**
- Cryptographers must have good **knowledge of database architecture**.
- Cryptographers must understand complicated mathematical theory and apply concepts and techniques to encryption algorithms
- A Cryptographers must be Familiar with data structures and algorithms remains essential, as do advanced mathematics skills.

2.4.2 Non-Functional Requirements

- The GUI of the system will be user-friendly.
- The data that will be shown to the users will be made sure that it is correct and is available for the time being.
- The system will be flexible to changes.
- The system will be extended for changes and to the latest technologies.
- Efficiency and effectiveness of the system will be made sure.
- The performance of the system will be made sure

2.4.3 Performance Requirements

System Parameters

The experiments are conducted using 3500+ AMD 64bit processor with 1GB of RAM. The simulation program is compiled using the default settings in .NET 2003 visual studio for C# windows applications. The experiments will be performed couple of times to assure that the results are consistent and are valid to compare the different algorithms.

Experiment Factors

To evaluate the performance of the compared algorithms, the parameters that the algorithms must be tested for must be determined.

Since the security features of each algorithm as their strength against cryptographic attacks is already known and discussed. The chosen factor here to determine the performance is the algorithm's speed to encrypt/decrypt data blocks of various sizes.

Simulation Procedure

By considering different sizes of data blocks (0.5MB to 20MB) the algorithms were evaluated in terms of the time required to encrypt and decrypt the data block. All the implementations were exact to make sure that the results will be relatively fair and accurate.

2.4.4 Security Requirements

Security Requirements, these are security services that needs to be achieved by the system under inspection. Examples could be authentication, authorization, backup, server-clustering, etc. This requirement artifact can be derived from best practices, policies, and regulations.

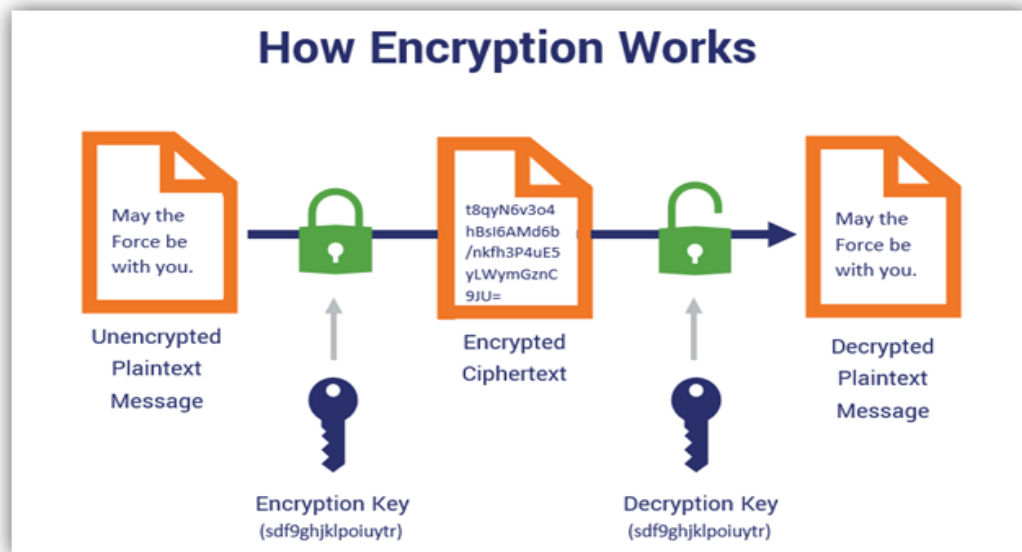
Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents

The simplest method uses the symmetric or "secret key" system. Here, data is encrypted using a secret key, and then both the encoded message and secret key are sent to the recipient for decryption. The problem? If the message is intercepted, a third party has everything they need to decrypt and read the message. To address this issue, cryptologists devised the asymmetric or "public key" system. In this case, every user has two keys: one public and one private. Senders request the public key of their intended recipient, encrypt the message, and send it along. When the message arrives, only the recipient's private key will decode it — meaning theft is of no use without the corresponding private key.

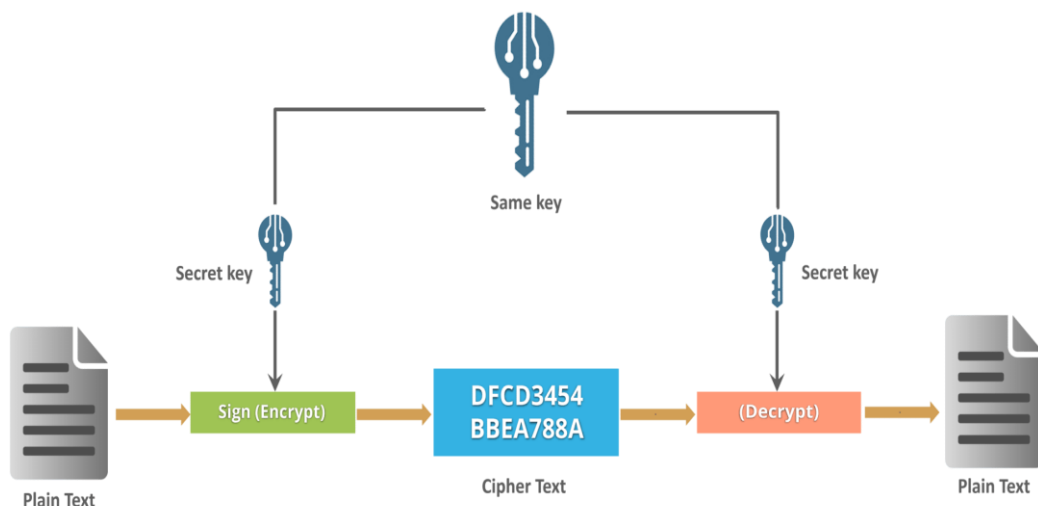
3. System Design

3.1 Design constraints

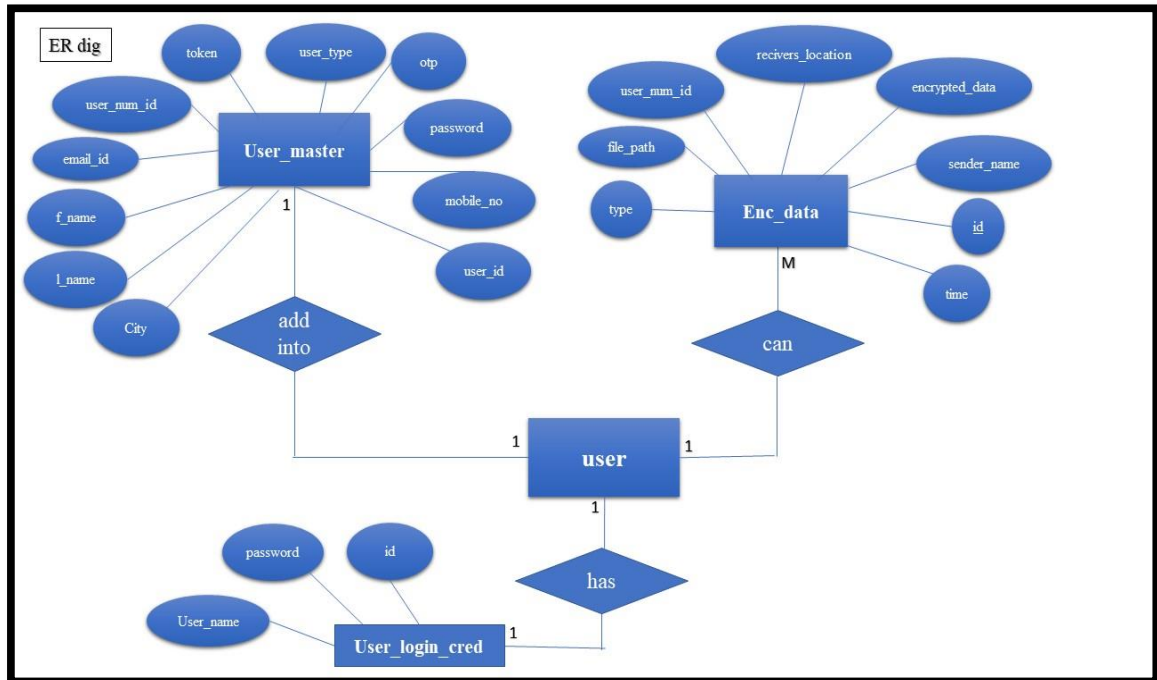
Steps of security System using cryptography Applications



cryptography Approach

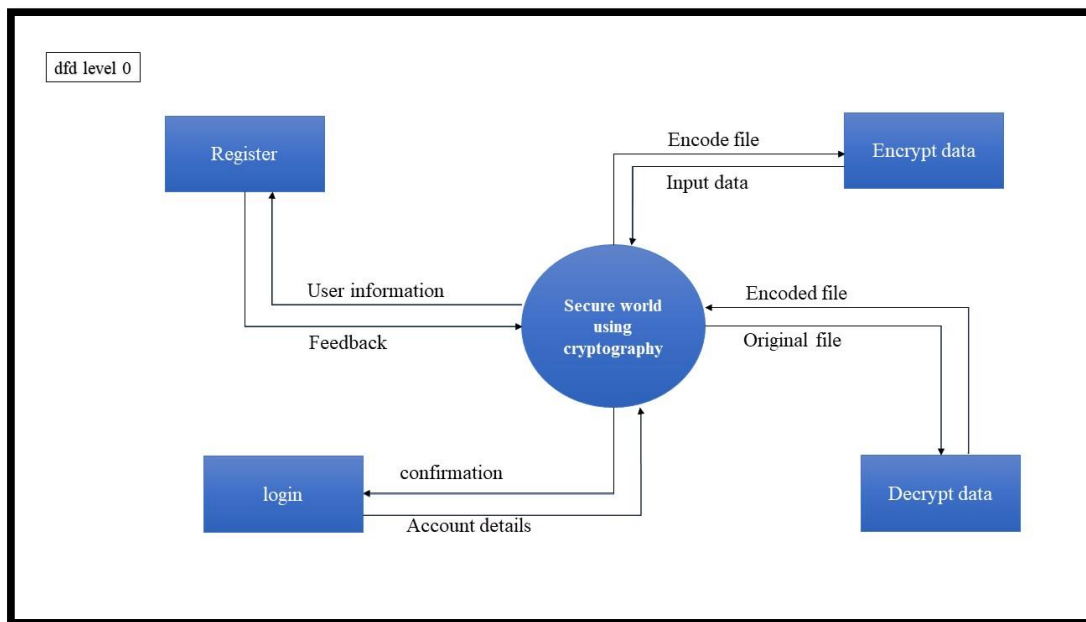


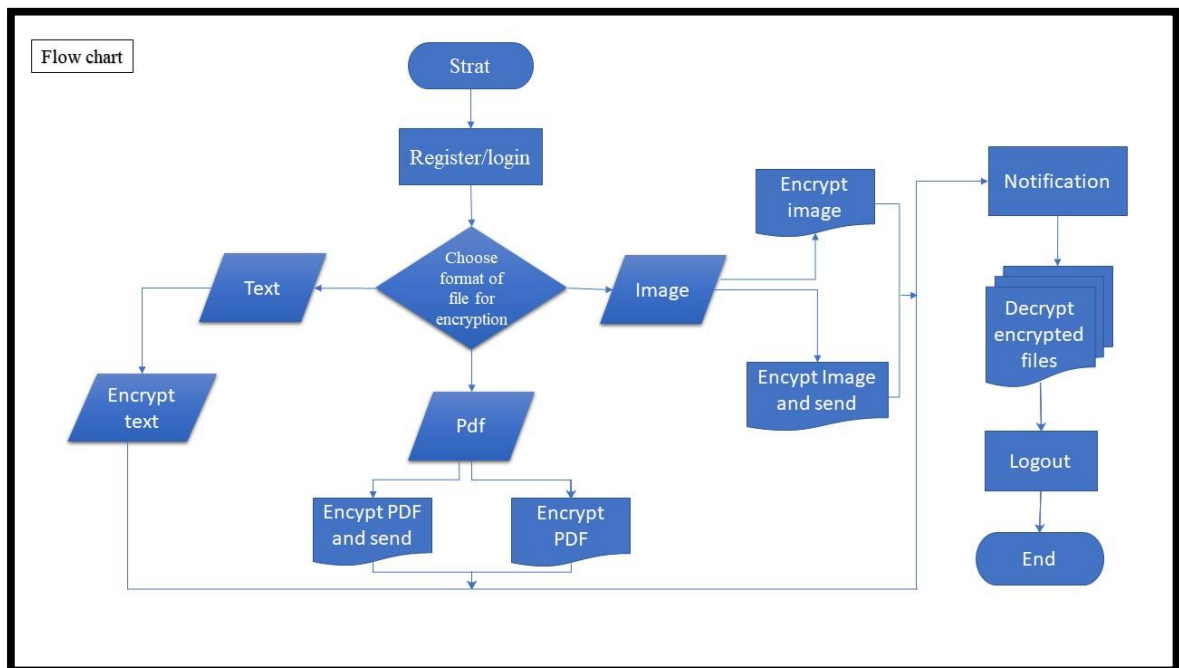
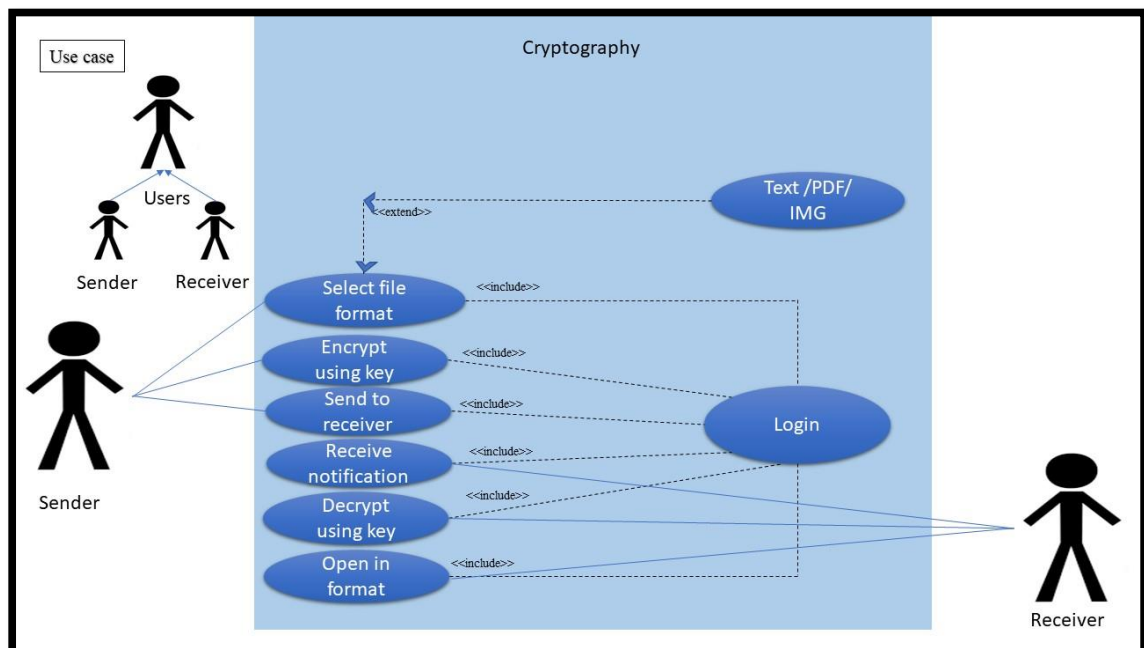
3.2 ER Diagram



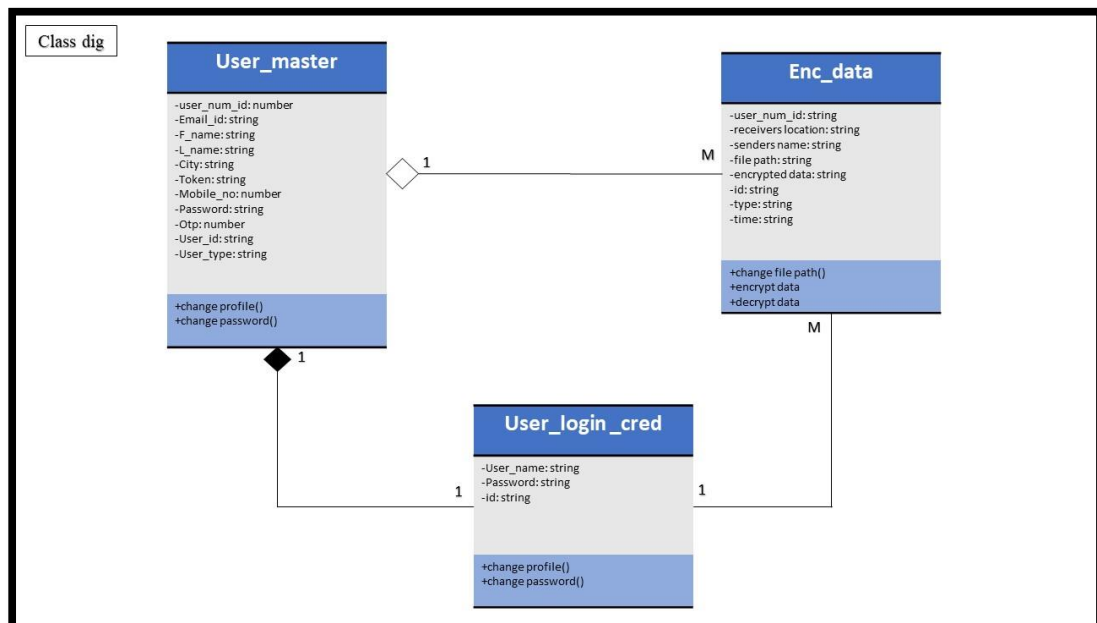
3.3 System Model: DFD

0th Level DFD:

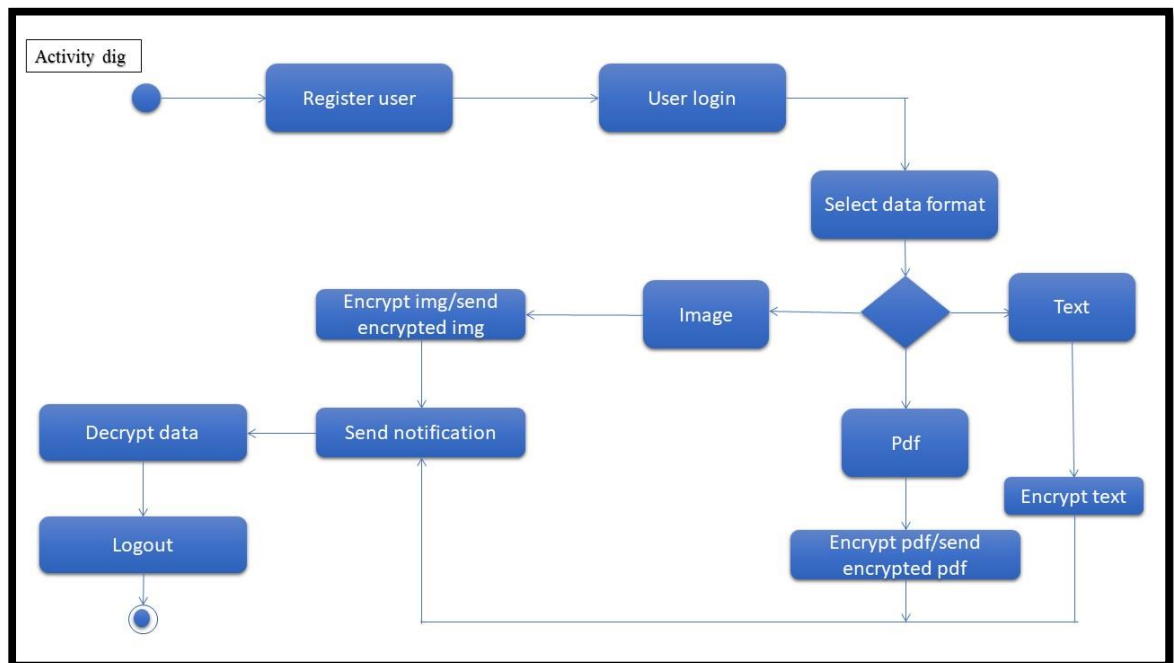


Flow chart:**3.4 Use case**

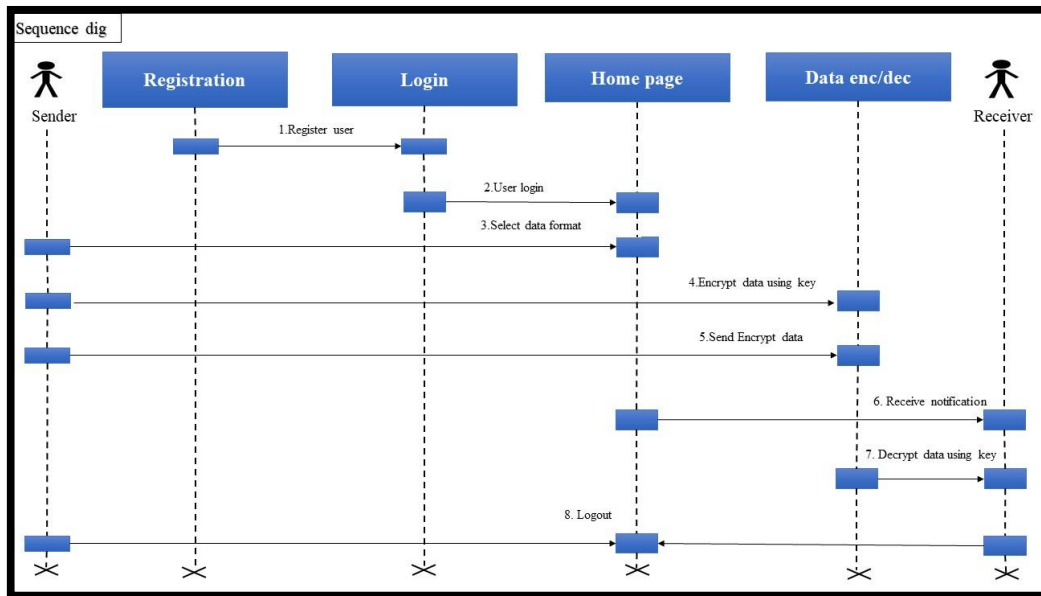
3.5 Class Diagram



3.6 Activity Diagram



3.7 Sequence Diagram



3.8 Data Dictionary

Dataset:

Table Name: **user_master**

Description: Contains the data of User

Primary Key: id

Field	Data Type	Constraints	Data Description
user_num_id	int (40)	Primary Key	Its store id of user provided by system,
user_id	varchar (20)	Not null	Its store Id of user
email_id	varchar (40)	Not null	Its store Email of user
mobile_no	Number (10)	Not null	Its store Mobile No. of user
f_name	varchar (20)	Not null	Its store first name of user
l_name	varchar (20)	Not null	Its store last name of user
token	varchar (20)	Not null	Its store automatically generated token of user
city	varchar (100)	Not null	its store city of user

user_type	varchar (20)	Not null	Its store type of user
Password	Varchar (20)	Not null	Its store encrypted password of user
otp	Number (4)	Not null	Its store Automatically system generated otp

Dataset:Table Name: **enc_data**

Description: Contains the encrypted data of User

Primary Key: id

Field	Data Type	Constraints	Data Description
id	int (100)	Primary key	Its store id of user
encrypted_data	varchar (20)	Not null	Its store encrypted data of user
sender_name	varchar (40)	Not null	Its store senders name
user_num_id	int (40)	Primary Key	Its store id of user provided by system
file_path	varchar (20)	Not null	Its store file path in system
Type	varchar (20)	Not null	Its store type of file
Receivers' location	varchar (20)	Not null	Its store automatically generated location of receiver
Time	varchar (100)	Not null	its store time of encryption

Dataset:

Table Name: user_login_cred

Description: Contains the login info of User

Primary Key: id

Field	Data Type	Constraints	Data Description
Id	varchar (255)	Primary key	Its store id of user
username	Varchar (255)	Primary Key	Its store name of user
Password	Varchar (255)	Not null	Its store encrypted password of user

3.9 User interfaces

An Interface is a specification that identifies a related set of properties and methods to be implemented by a class. In other words, a given class agrees to support this specification when it implements that interface. The interface is simply the definition of the properties and methods, and the class that implements that interface has the actual code for each of those defined properties and methods. In Typescript, you can use the interface itself as a data type. Interfaces in Typescript are a development time only concept, they are not included in the final JavaScript after the build process.

Angular leverages Typescript, developers can make use of strong typing. This is a big help during development, since your IDE will help catch errors before even building the application. That way, you can fix issues as soon as the IDE gives a notification that something went awry. Taking this concept one step further is the use of Interfaces. Although JavaScript itself does not have Interfaces, Typescript does. Interfaces are very common in object-oriented programming languages like Java, PHP, and C#. With Typescript, we can now also use them on the front end.

4. Implementation details

The Encryption Process

The data encryption implementation has the following steps:

- The process of encryption begins by converting the text to a pre-hash code. This code is generated using a mathematical formula.
- This pre-hash code is encrypted by the software using the sender's private key.
- The private key would be generated using the algorithm used by the software.
- The encrypted pre-hash code and the message are encrypted again using the sender's private key.
- The next step is for the sender of the message to retrieve the public key of the person this information is intended for.

The Decryption Process

The data decryption process has the following steps:

- The recipient uses his/her private key to decrypt the secret key.
- The recipient uses their private key along with the secret key to decipher the encrypted pre-hash code and the encrypted message.
- The recipient then retrieves the sender's public key. This public key is used to decrypt the pre-hash code and to verify the sender's identity.

4.1 Software/Hardware Specifications

Hardware-Based Cryptography	Software-Based Cryptography
1. Uses dedicated hardware, thus much faster to execute.	1. Uses shared hardware, thus slower to execute.
2. Not dependent on the operating system. Supported by dedicated software to operate the hardware.	2. Dependent on the security levels and features of the operating system and supported software.
3. Can use factory provisioning and securely store keys and other data in dedicated secure memory locations.	3. No dedicated secure memory locations available. Thus, susceptible to stealing or manipulation of keys and data.
4. Maxim's hardware implementations have protections built in against reverse-engineering, such as PUF (ChipDNA).	4. Software implementations can be easier to reverse-engineer.
5. In a hardware system, special care is taken to hide and protect the vital information, such as private keys, to make it much more difficult to access.	5. In a general-purpose system where software cryptography is implemented, there are more ways to snoop to and access vital information. An example would be intercepting the private key in transit within the computer's system.

5.Outputs and Reports Testing

5.1 Unit Test:

Unit testing incorporates the configuration of analyses that supports that the actual project rationale is met appropriately, and that the framework inputs generate subsequent reliable outputs. All the branches of code and internal functionalities should be acknowledged and tested. Before the application goes live, unit testing is an approach that ensures the functionalities of individual programming units of the application. This is an essential test that relies upon the data that is sent as input or parameters and the method of invoking the individual unit. Unit tests perform key tests at fragment level and test a specific business strategy, application, as well as framework setup. Unit tests ensure that each unit for a business strategy 60 performs precisely to the reported points of interest and contains detailed sources of information and results that are expected. Unit testing example: Unit testing forms as a vital aspect of an integrated code snippet. This testing is ought to be performed before integration testing in the product lifecycle. For instance, when a banking application is developed, the individual components, like a savings account or checking account modules, need to unit tested. Unit testing includes the following two important stages: Test strategy and approach. Field testing is usually performed physically, whereas software testing can be performed virtually.

Test objectives: All field entries should be working legitimately. Pages should be derived from the distinguishable link connection. The actual entry screens or messages or actions should not be altered.

Features to be tested include

- check that the sections have the right configuration
- ensure that no copy of sections will be allowed
- make sure that all connections lead the client to the right or correct page

5.2 Integration Test: -

Integration tests are expected to test the programming components in conjunction with other components to make sense of whether they truly continue running as one framework. Testing is event driven and is more concerned with the crucial effects of fields on screens. Integration tests display results disregarding the way that the sections were solely satisfied, as showed up by successful unit testing, the integration of segments is correct and reliable. This testing is especially used to uncover the issues that rise out of the integration of individual programming parts or components.

5.3 Test cases:

To verify login

Test Case ID	Test Case Name	Sub Test Case ID	Steps to Execute	Expected Result	Actual Result	Pass/Fail
TC_1	To Verify Login Page	TC_001	Keep username and password blank and click login	Display error message for entering username and password	Displays error message	Pass
		TC_002	Enter username correct and password incorrect and click login	Display error message invalid login details.	Displays error message	Pass
		TC_003	Enter username incorrect and password correct and click login	Display error message invalid login details	Displays error message	Pass
		TC_004	Enter username and password correct	Display the dashboard	Displays the dashboard	Pass
		TC_005	Click forgot password link	Display forgot password page	Display forgot password window	Pass

For Encrypting Data

Test Case ID	Test Case Name	Sub Test Case ID	Steps to Execute	Expected Result	Actual Result	Pass/Fail
TC_2	To Encrypt Data	TC_001	Select Data Format	Go to the selected format section	Jump on a selected format data window	Pass
		TC_002	Keep the fields blank (message, secure key, receiver's userid)	Show error all fields are compulsory	Pop up window with error message	Pass
		TC_003	Enter wrong username	Display message user not found	Popup window with error	Pass
		TC_004	Fill all the fields & click on send message button	Encrypted data send to requested user id	Encrypted Data successfully sent	Pass

For Decrypting Data

Test Case ID	Test Case Name	Sub Test Case ID	Steps to Execute	Expected Result	Actual Result	Pass/Fail
TC_3	To decrypt data	TC_001	Check the notification tab	The decrypt data sent by sender should appear in notification tab of receiver	Receive notification in same tab	Pass
		TC_002	Click on view option	The window should jump on decrypt data section	Decrypt data section window appear	Pass
		TC_003	Enter wrong security key n try to decrypt the data	The system should throw error incorrect key	Error popup Incorrect key	Pass
		TC_004	Enter right key n try to decrypt message	Data should decrypt	Show Decrypted data	Pass

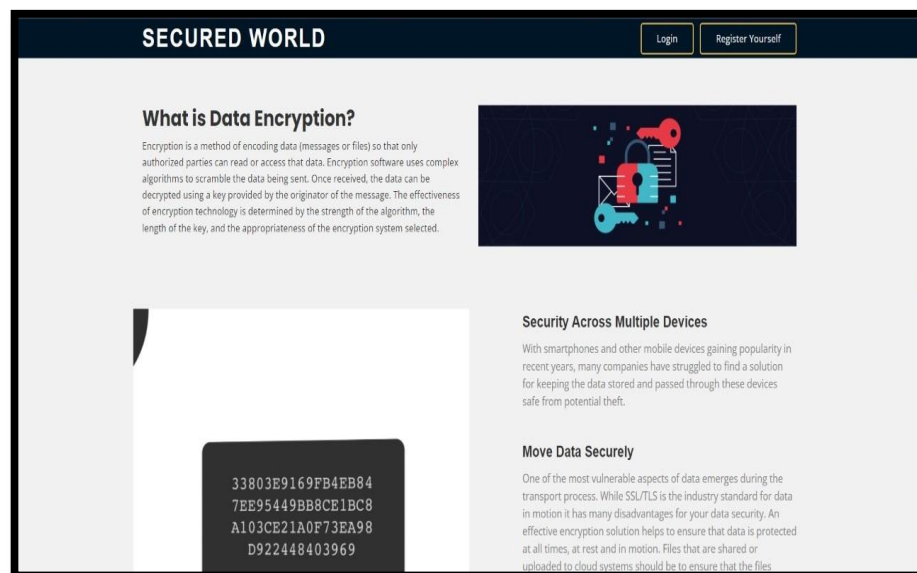
5.5 Sample Input & Output Screen

Fig.1 This is index page where user can find login or registration form



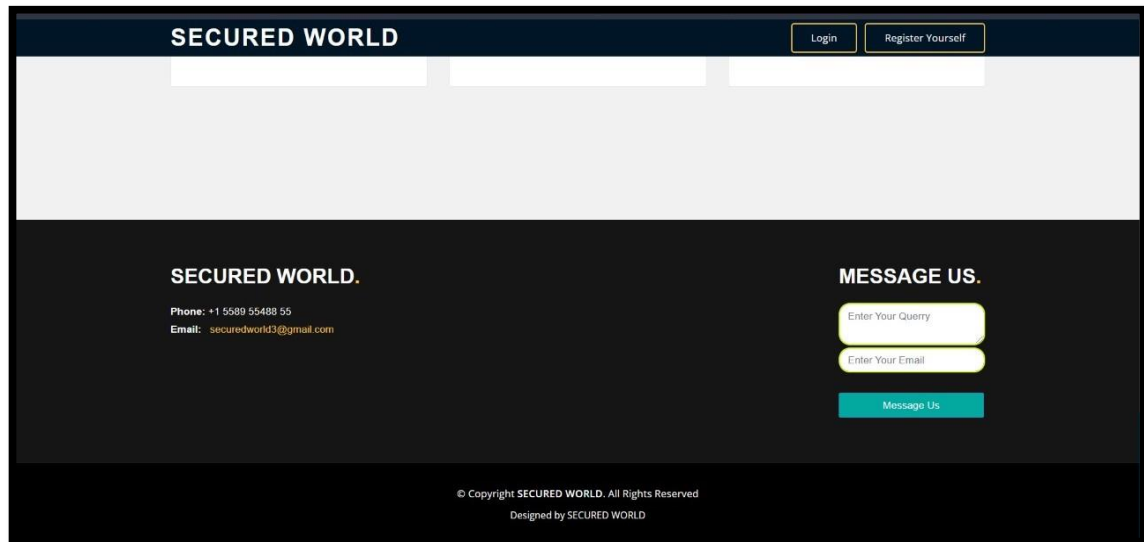
(Fig.1)

Fig.2 From this page u can find the requirements as well as pros of the system



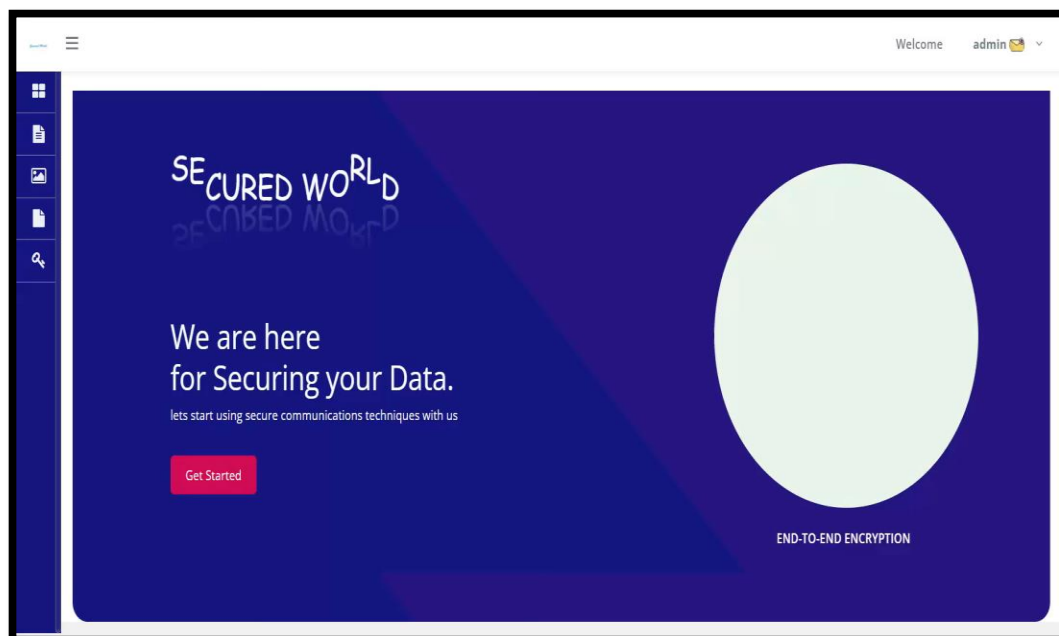
(Fig.2)

Fig.3 From this page you can contact for help in query's



(Fig.3)

Fig.4 Here we can select format of the file from tab, we can check the notifications, we can generate a key.



(Fig.4)

Fig.5 Here is a profile of a user. User can check or modify details and can update profile of themselves here.

The screenshot displays the 'Profile Settings' interface. On the left, a sidebar contains navigation links: Home, Text, Image, and Documents. The main content area features a user profile card for 'admin' with a profile picture and email 'aadeshpatil650@gmail.com'. Below the card is a 'Change Profile Pic' button. To the right, the 'Profile Settings' form contains the following fields: Name (Aadesh), Surname (Patil), Email Id (aadeshpatil650@gmail.com), Mobile No. (9960776997), City (pune), and State (maharashtra). A green 'submit' button is located at the bottom right of the form.

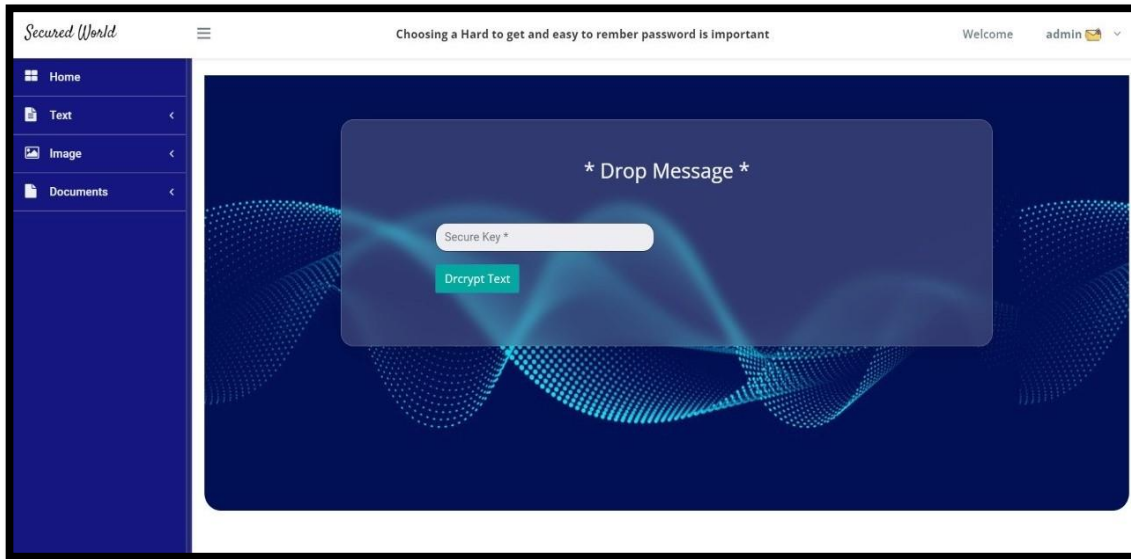
(Fig.5)

Fig.6 Here user can encrypt the data which is in text format. In this format user can send the data to multiple users. User can also check if the receiver's id is present in system or not.

The screenshot shows the '* Drop Message *' form. The sidebar on the left has 'Text' selected, with a sub-option 'Text Encryption'. The form area has a dark blue background with a glowing effect. It contains three input fields: 'Your Message *', 'Receiver UserId *', and 'Secure Key *'. Below the 'Receiver UserId *' field are two buttons: 'Check User Details' (yellow) and 'Send Message' (red). At the bottom, there is a checkbox labeled 'Do You Want to Send to Multiple Users.'.

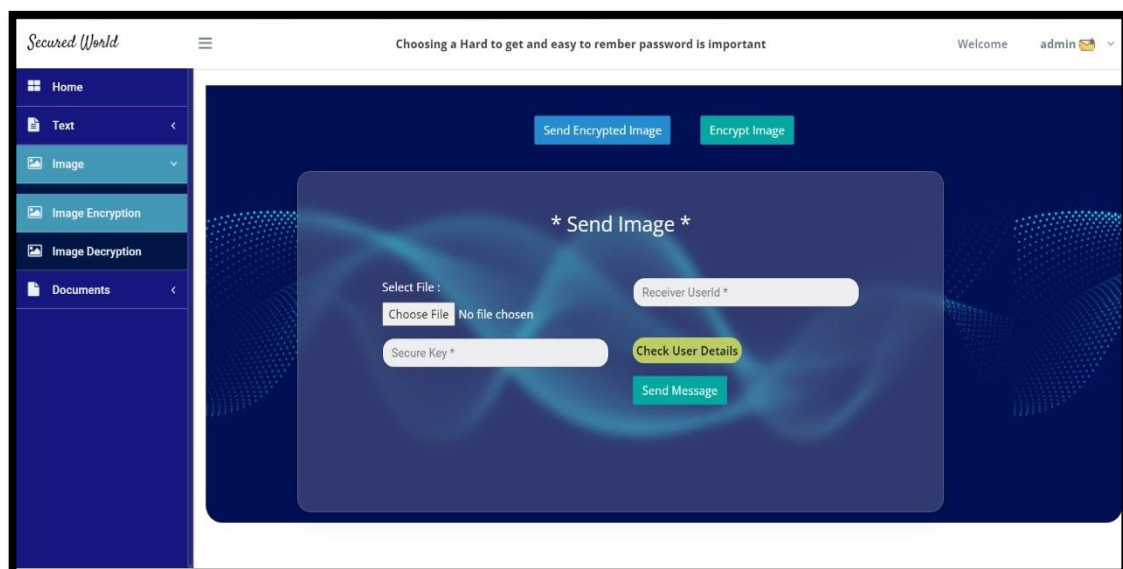
(Fig.6)

Fig.7. Here user can decrypt the data which is received in notification tab at receive end. User can the text using the secure key.



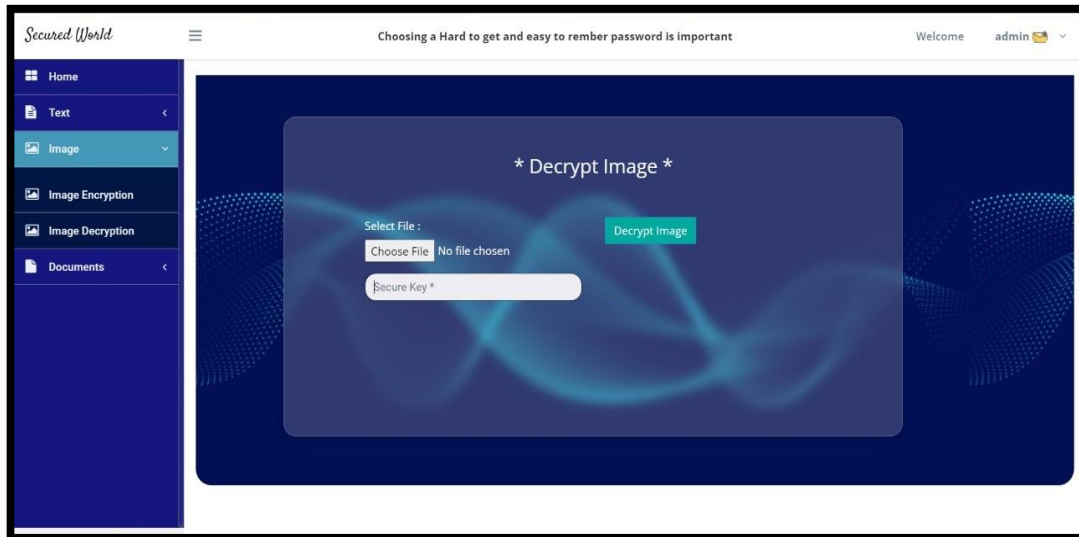
(Fig.7)

Fig.8 Here user can encrypt the data which is in Image format. User can also check if the receiver's id is present in system or not. Users have a choice to send the encrypted data or user can encrypt the data at a time of execution.



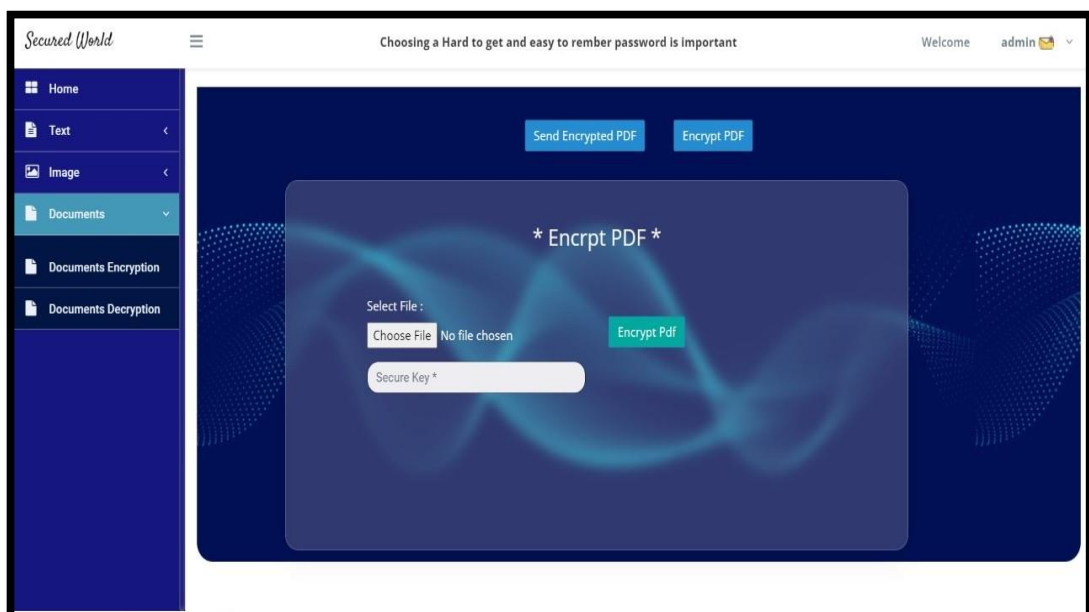
(Fig.8)

Fig.9 Here user can decrypt the data which is received in notification tab at receiver end. User can decrypt the Image using the secure key.



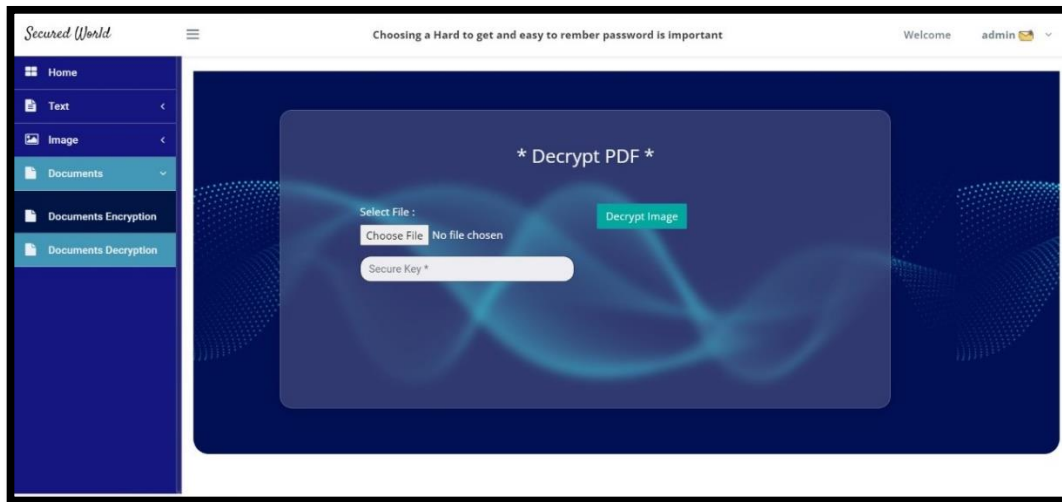
(Fig.9)

Fig.10 Here user can encrypt the data which is in PDF format. User can also check if the receiver's id is present in system or not. Users have a choice to send the encrypted data or user can encrypt the data at a time of execution.



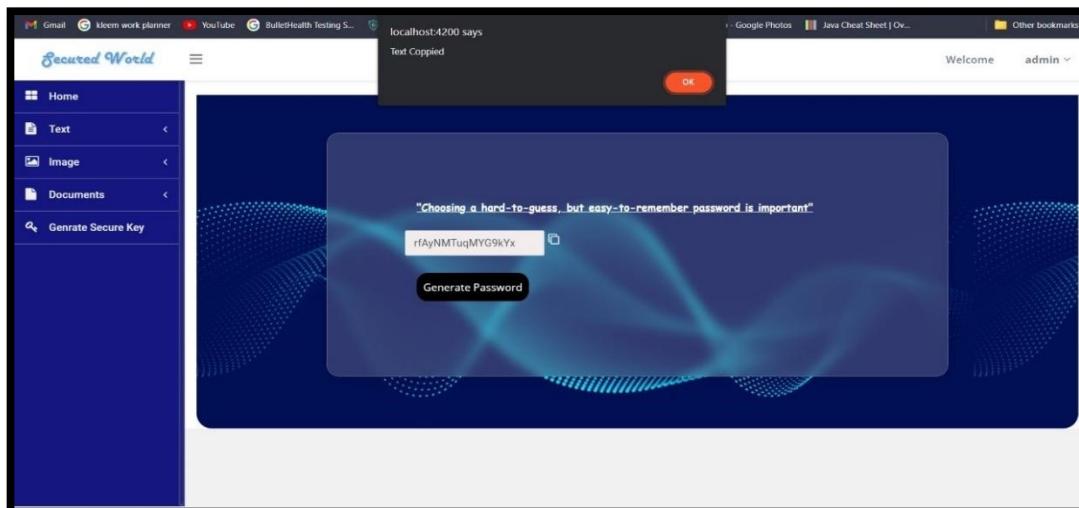
(Fig.10)

Fig.11 Here user can decrypt the data which is received in notification tab at receiver end. User can decrypt the PDF using the secure key.



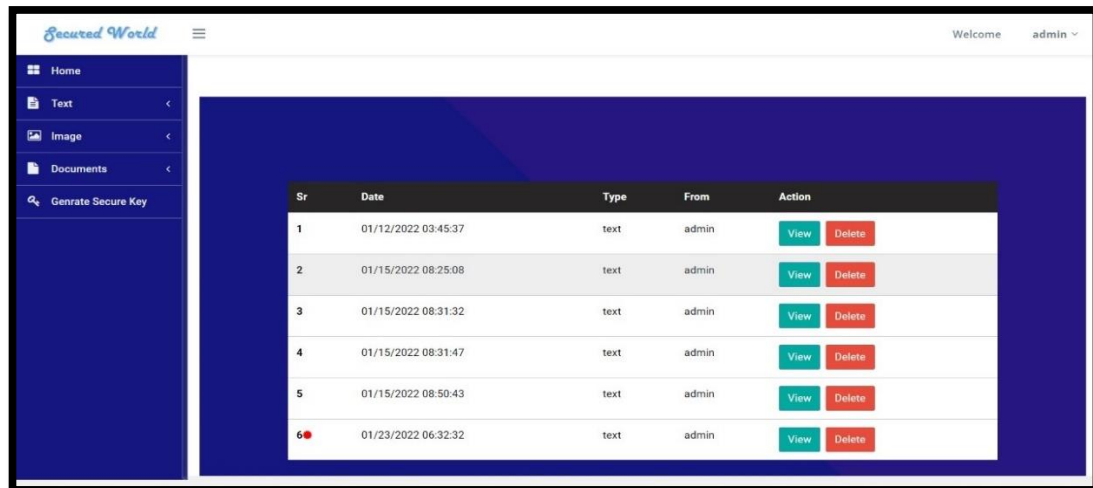
(Fig.11)

Fig.12 User can generate secure key.



(Fig.12)

Fig.13 When sender sends the encrypted file to receives notification in this tab. User can view or delete the data.

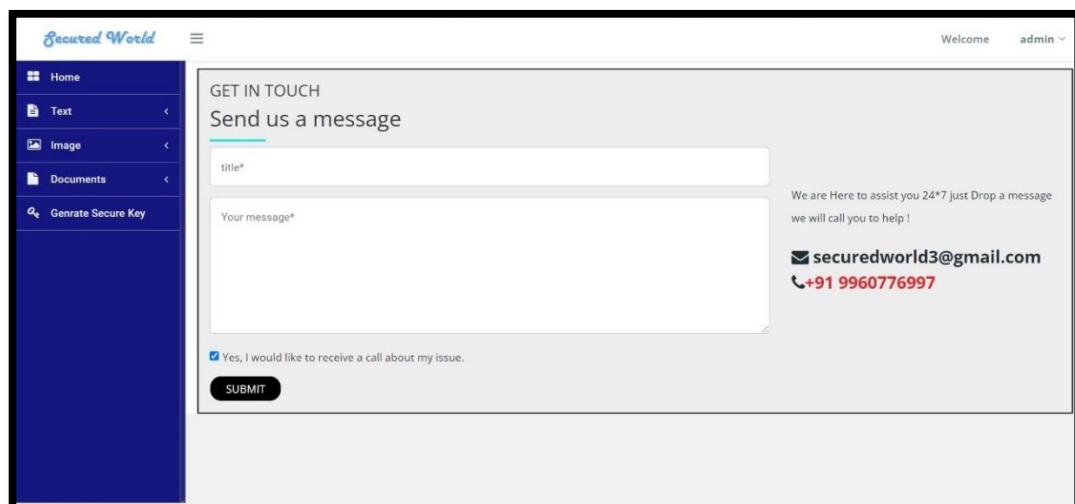


The screenshot shows the 'Secured World' application interface. On the left is a dark blue sidebar with navigation links: Home, Text, Image, Documents, and Genrate Secure Key. The main content area has a dark blue header with the application logo and a user profile 'Welcome admin'. Below the header is a table with the following data:

Sr	Date	Type	From	Action
1	01/12/2022 03:45:37	text	admin	View Delete
2	01/15/2022 08:25:08	text	admin	View Delete
3	01/15/2022 08:31:32	text	admin	View Delete
4	01/15/2022 08:31:47	text	admin	View Delete
5	01/15/2022 08:50:43	text	admin	View Delete
6	01/23/2022 06:32:32	text	admin	View Delete

(Fig.13)

Fig.14 From this page you can contact for help and queries.



The screenshot shows the 'Secured World' application interface with a 'GET IN TOUCH' section. The form includes a title input field, a message input field, and a checkbox for receiving calls. The contact information provided is:

We are Here to assist you 24*7 just Drop a message we will call you to help !

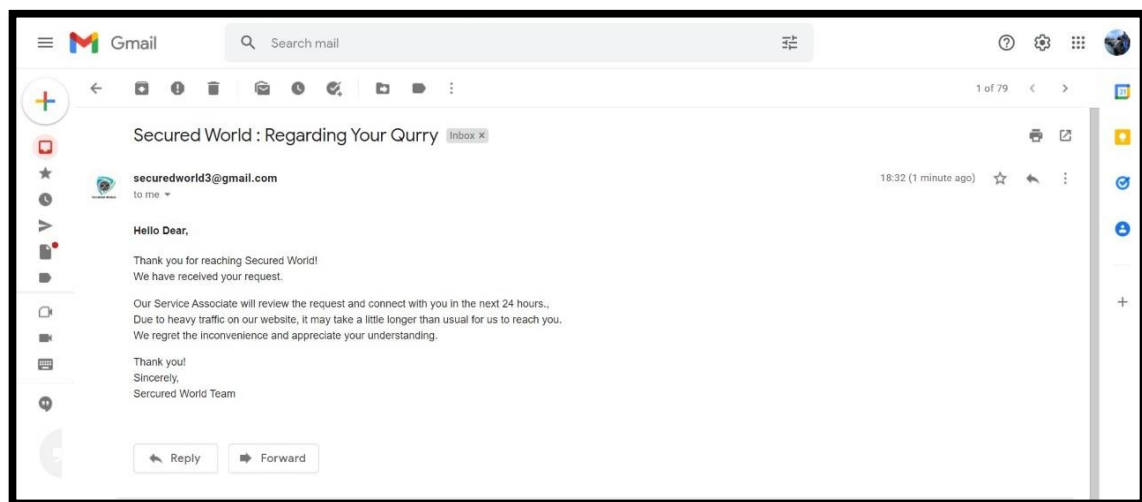
securedworld3@gmail.com
 +91 9960776997

☒ Yes, I would like to receive a call about my issue.

[SUBMIT](#)

(Fig.14)

Fig.15 After user submit support form user will receive this kind of mail



(Fig.15)

6. Conclusion

The purpose of this section is to present how cryptography can be used to implement security in the Web. It starts with a list of challenges for protecting information, continues with the presentation of the basic cryptographic algorithms and protocols, presents the Secure Sockets Layer protocol, and concludes with an example of how cryptography is used in a commercial transaction on the Internet.

From a technical point of view, cryptography is the solution to many of the security challenges that are present on the Internet. The technology exists to solve most of the problems. However, there are several issues that have obstructed the widespread use of cryptography on the Internet. First, cryptography, as a science, faces a difficult problem. Most of the algorithms cannot be proven secure. For this reason, there is suspicion around many of the cryptographic algorithms. Another aspect is related to the intellectual property associated with the algorithms. Most algorithms are patented, and only some companies have licensed them for use.

Finally, cryptography can be used to harm society. Governments are concerned that encryption will make law enforcement and national security goals more difficult to achieve. For example, terrorists could communicate information over the Internet using encryption that law enforcement agencies could not decrypt. Therefore, some governments, such as the U.S., have regulated the export of software containing encryption algorithms. This is a topic of debate, pitting governments against the right to free speech.

However, the following year a different District Court made an opposite ruling in a different case. Daniel Bernstein, while a Ph.D. candidate at the University of California, was told by the U.S. government that he had to register as an arms dealer under the International Traffic in Arms Regulation to publish a cryptographic program. Bernstein sued. In August 1997 the Federal District Court in San Francisco ruled that export restrictions on encryption are "an unconstitutional prior restraint in violation of the First Amendment". According to the Justice department, the larger issue of exporting cryptographic algorithms remains unresolved.

The current trend in society indicates that cryptography is gaining importance. One day cryptography may be widely used throughout the Internet: for electronic mail, for sending documents that are sold over the Web, and even perhaps for all network communication between routers or switches on the Internet. The use and debate on cryptography promises to be prominent for many more years.

7. Future enhancement

- We can use two step authentications for login data to provide extra security
- We can add video and audio encryption/decryption methods in this system
- We can give choice to user for cryptography and steganography methods
- We can update the changes in system suggested by users
- We can add some setting for better GUI (themes)
- working on android, iOS application for the same System
- sender will see the descriptors' location in app itself

8. Bibliography and References

For information on the politics of cryptography and privacy, see these sources:

On the web:

- www.epic.org - Electronic Privacy Information Center
- www.crypto.org - Internet Privacy Coalition
- www.eff.org - Electronic Frontier Foundation
- www.privacy.org - Great information resource about privacy issues
- www.cdt.org - Center for Democracy and Technology
- www.philzimmermann.com - Phil Zimmermann's home page, contains useful info

For technical aspects of cryptography, see the following sources.

On the web:

- The PGP International home page
(Nice FAQ, and PGP source code - the best PGP site on the web)
- www.nist.gov/aes
The NIST Advanced Encryption Standard
(Perhaps the most interesting project in crypto in recent years)

Books:

- [Practical Cryptography](#)
Niels Ferguson and Bruce Schneier, John Wiley & Sons, 2003
ISBN 0-471-22357-3
(If you can only read one book on crypto, this is it)
- [Applied Cryptography, 2nd edition](#)
Bruce Schneier, John Wiley & Sons, 1996
ISBN 0-471-12845-7
(Before Practical Cryptography came out, this was the one book you needed)
- [Handbook of Applied Cryptography](#)
Alfred Menezes, Paul van Oorschot, and Scot Vanstone, CRC Press, 1996
ISBN 0-8493-8523-7